WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
HEIDI L. KEEFE (State Bar No. 178960)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
RICHARD D. MC LEOD (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

| | |
|---|---|
| INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,<br>Plaintiff,<br>v.<br>MICROSOFT CORPORATION, a Washington corporation,<br>Defendant. | CASE NO. C01-1640 SBA (MEJ)<br><br>**MICROSOFT'S MARKMAN BRIEF** |
| MICROSOFT CORPORATION, a Washington corporation,<br>Counterclaimant,<br>v.<br>INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,<br>Counter Claim-Defendant. | The Honorable Saundra B. Armstrong |

## TABLE OF CONTENTS

## CASES

**STATUTES/OTHER**

## I. INTRODUCTION

The claims must be read in light of the entire 900+ page "Big Book" patent application and, in particular, its 115 page "Summary of the Invention." This Summary of the Invention makes literally hundreds of statements touting the "important," "fundamental," "critical," and required features, capabilities and purposes of the "present invention." The Summary further defines this "invention" (which it expressly names "VDE") by distinguishing it from the allegedly "limited" and rigid solutions of others. All of these are required aspects of the "present invention," not merely optional features of a "preferred embodiment." As such, the claims must be read to include these "invention" features.

### A. A Valid Claim Must Reflect This "Invention"

The Big Book's Summary of the Invention is InterTrust's elephant in the corner. The claim constructions urged by InterTrust are devoid of any of the required features of the "invention." InterTrust acts as if this "invention" simply did not exist. For example, the Big Book touts that VDE is able to prevent (not merely detect) all unauthorized access to protected content. Yet, InterTrust uniformly ignores this core promise of VDE security in its claim construction proposals, and instead urges that merely detecting misuse of content is sufficient.

InterTrust's whole approach is wrong. To ignore a patent's described "invention" when construing a patent claim, is contrary to patent law. "What is claimed by the patent application must be the same as what is disclosed in the specification; otherwise the patent should not issue." Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., 535 U.S. 722, 736 (2002). Thus, "it is fundamental that claims are to be construed in the light of the specifications and both are to be read with a view to ascertaining the invention." Adams v. United States, 383 U.S. 39, 49 (1966) (holding that patent claims required what the patent identified as an "object" of the "invention," even though the claims did not expressly recite that feature). Here, the Big Book's Summary of the Invention is critical to "ascertaining the invention."

**B. These Twelve Claims Do Invoke This "Invention"**

InterTrust's patent claims invoke the required features of the alleged "invention" in at least three ways.[1]

**VDE Claim Terms**: First, many of the key claim terms are VDE terms having special meanings in the VDE context. For example, the Big Book uses several general-sounding, functional terms (often a coined phrase) as short-hand labels for specific VDE mechanisms, such as "control," "container," "protected processing environment," and "virtual distribution environment." In these patents, a "control" is not whatever can exercise some kind (any kind) of control over something else; a "container" is not whatever can contain something; a "protected processing environment" is not any processing environment which is protected; and a "virtual distribution environment" is not any distribution environment which is virtual. Rather, these terms have special VDE meanings. For example, the Big Book defines its "virtual distribution environment" as a special breed: "The present invention provides a new kind of 'virtual distribution environment' (called 'VDE' in this document) that secures, administers, and audits electronic information use." ('193 2:24-27). These claim terms must be construed in their specific VDE sense, not some general sense divorced from the described "invention." (See Maier Decl. at 21-35.)

**Vague Claim Terms**: Second, most of the key claim terms are quite vague. These terms would deprive the claims of required clarity unless they are refined in light of the disclosed "invention." For example, ten of the mini-Markman claims use the terms "secure," "securely," and/or "protected." These claims do not specify how to distinguish a secure [something] from a non-secure [something], etc. Whether a "container" is "secure," for example, depends on the context, such as what is being protected, against what threats, for how long, and to what degree. (See Tran Decl. (Public) (assembling references); Keefe Decl. (assembling testimony: e.g., Shear Depo. at 100:19-101:23; Sibert Depo. at 97:20-25, 29:8-11); and the first Declaration of John

[1] Any claim that fails to invoke its specification's "invention" is invalid under 35 U.S.C. § 112, ¶ 1's "written description" requirement and ¶ 2's "regards as the invention" requirement. (See infra, Section V).

Mitchell (filed March 17, 2003).) As the claims do not expressly provide this required context, resort must be had to the disclosed "invention."[2] Many other claim terms also are sorely in need of definition from the specifications. (Cf. InterTrust Br. at 9:2-18).

**VDE Claim Promises**: Third, a core "invention" promise is the ability to prevent unauthorized access to (and use of) protected digital content notwithstanding myriad threats—identified in the Big Book—attempting to break or bypass that protection. (E.g., '193 221:19 et seq.) Each of the mini-Markman claims invokes this core VDE promise by promising to protect some content, process, and/or component. These promises of protection are unqualified. The claims identify no threat against which their promised protections are ineffective. The Big Book describes only one system for providing such "true" protection against these threats, and that is the complete VDE "invention." In other words, by requiring the promised protections supposedly afforded by the "invention," these claims invoke the required features of that "invention."

**C. These Claims Demand Precise Constructions, True To The "Invention"**

As InterTrust says, its proposed constructions are simple. They are simple, however, because (1) they are unfettered by the disclosed "invention" and its required capabilities and features touted in the Big Book's Summary of the Invention, (2) they treat the claims' specific VDE terms as general, non-VDE terms, (3) they ignore what each claim promises, and (4) they often are so vague as to be essentially meaningless.

InterTrust challenges Microsoft's constructions as complex. They are complex, because they honor precisely what the Big Book describes as the many required features of the "present invention." A proper construction of these claims necessarily is lengthy due to the sheer number of features the Big Book identifies as being "important" to its "invention." These required features are not "detailed limitations from specified embodiments," as charged by InterTrust (InterTrust Br. at 1:19-20), but rather the self-described "important" features of the "invention."

Simplicity and brevity are worthy goals in claim construction. But, they do not trump clarity and accuracy. Skilled persons faced with these claims would not dismiss any required

[2] Here, InterTrust's specification is internally inconsistent and, in some ways, makes the scope of the claims even less clear. Consequently, Microsoft has moved for summary judgment of claim indefiniteness.

aspect of the Big Book's "invention." The sheer size of the Big Book should not frustrate the rules of claim construction, leave the public or jury guessing about a claim's precise boundaries, or divorce the claims from what the patent applicants touted as their "present invention."

## II. SUMMARY OF ACCOMPANYING DECLARATIONS

The parties agree that this subject cannot be fully addressed in a 40-page brief. This Brief addresses some important features of the "invention" and some of the primary claim construction disputes. It is supplemented by the JCCS, and by the following declarations:

**VDE's Features**: The Declaration of Prof. David Maier, of Oregon Graduate Institute, describes the Big Book's "invention" and its mandatory features. To illustrate the operation of this "invention," he also explains the Big Book's only detailed example of how VDE handles a request to read protected content. Prof. Maier also describes some of the inconsistencies in the Big Book, including some that contradict passages cited by InterTrust.

**"Security" And The Claims**: Prof. John Mitchell, of Stanford, submitted a report on Microsoft's pending motion for summary judgment of claim indefiniteness. That report also pertains to claim construction. It explains how the label "secure" is "multi-dimensional, highly contextual, relative (i.e., a matter of degree), and subjective unless objectively defined." In his second Declaration, Prof. Mitchell explains how the "security" protections promised by the "invention" would have affected a skilled person's understanding of certain claim terms.

**Prosecution History**: Mr. Alexander summarizes portions of the Patent Office files for these patents and explains the relationships between the patents. Included is the Patent Office's statement (set forth with its reasons for allowing the '193 patent to issue) that InterTrust had filed "a series of applications generally relating to a virtual distribution environment."

**Deposition Testimony**: In opposing Microsoft's motion to stay certain discovery, InterTrust argued that the parties' own uses of the claim terms are important to claim construction. (InterTrust Opp. to Microsoft's Motion for Stay at 9-10 & n. 9 (October 1, 2002).) Microsoft has since deposed several InterTrust employees, former employees, licensees, and licensee candidates, as well as InterTrust's expert, Prof. Reiter. Their testimony confirms that

many key claim terms lack any precise meaning outside of VDE. Ms. Keefe's Declaration collects some of this testimony.

**Documentary Evidence**: Two Declarations by Xuan-Giang Tran submit documentary evidence supplementing the parties' joint submission of intrinsic evidence.

## III. THE BIG BOOK'S "INVENTION"

Microsoft asks the Court to construe each claim as requiring the disclosed "invention," as it has been distilled in Microsoft's global "claim as a whole" construction. (JCCS Exh. A, Row 86). Some of the important aspects of this "invention"—aspects which the Big Book cites to distinguish prior systems—are summarized below. (See also Maier Decl. at 5-14).

**Data Security and Commerce World**: The overall purpose of the "invention's" Virtual Distribution Environment (VDE) is for securing, administering, and auditing all security and commerce digital information within its multi-node "world." VDE guarantees to all participants in this VDE world that it can limit all access to, and use of, such security and commerce information, to authorized activities and amounts.

> "The **present invention provides a new kind of 'virtual distribution environment' (called 'VDE' in this document) that secures, administers, and audits electronic information use**. VDE also features fundamentally important capabilities for managing content that travels 'across' the 'information highway.'" ('193 2:24-28)
>
> "**The present invention** can provide a "unified," efficient, secure, and cost-effective system for electronic commerce and data security. This allows VDE to serve as **a single standard for electronic rights protection, data security, and electronic currency and banking**." ('193 7:9-14)
>
> "VDE is a cost-effective and efficient rights protection solution that provides a unified, consistent system for securing and managing transaction processing. **VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users.**" ('193 4:48-55)

(Alexander Decl. Exh. D at 24-1(C), 24-9(C), 24-1(F).) (Emphases added throughout this Brief, unless otherwise noted).

**Comprehensive Range of Functions**: The Big Book distinguishes its comprehensive "invention" from supposedly "limited" traditional systems that addressed only some aspects of data security and commerce.

> "**Content providers and distributors have devised a number of limited function rights protection mechanisms to protect their rights**. Authorization passwords and protocols, license servers, 'lock/unlock' distribution methods, and non-electronic contractual limitations imposed on users of shrink-wrapped software are a few of the more prevalent content protection schemes. In a commercial context, **these efforts are inefficient and limited solutions.**" ('193 3:1-9)
>
> "**Despite the attention devoted** by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies **to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems.**" ('193 2:13-22)

(Alexander Decl. Exh. D at 24-7(K), 24-4(V).)

**User-Configurable**: The "invention" governs access to and use of protected information with executable VDE "controls." These VDE controls are not built-in, fixed mechanisms. Rather, VDE allows its participants to create, modify, and merge these VDE controls, partly through a VDE-controlled negotiation process. For example, VDE purports to enable[3] a consumer to place limits on the amount of time or money that a participant (whether human or machine) can spend using the protected content, subject only to other users' "senior controls."

> "The **inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention.**" ('193 2:11-13)
>
> "The **configurability provided by the present invention** is particularly **critical for supporting electronic commerce**, that is enabling businesses to create relationships and evolve strategies that offer competitive value. **Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce** products (and services) that meet both basic requirements and evolving needs of most commerce applications." ('193 16:41-48)

---

[3] Throughout this brief, Microsoft describes various features described in the Big Book and other InterTrust patents. By reiterating what InterTrust patent documents say, Microsoft does not imply that those documents actually described a working system that could accomplish what they promised. In other words, Microsoft addresses what the patents purported to describe, not whether they actually enabled anything.

(Alexander Decl. Exh. D at 24-4(V), 24-4(W).)

**Flexible**: The Big Book further distinguishes its supposedly flexible system from rigid systems. For example, rather than requiring a VDE user to purchase an entire, pre-defined content package (e.g., an entire movie), the "invention" can permit a VDE user to purchase only user-defined increments of that information (e.g., her favorite scenes).

> "**Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.** VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, **VDE includes features that . . . support dynamic user selection of information subsets of a VDE electronic information product (VDE controlled content). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments** such as being required to select a whole information product or product section in order to acquire or otherwise use a portion of such product or section. . ." ('193 21:43-53; 22:32-38)
>
> "**VDE does not require electronic content providers and users to modify their business practices and personal preferences to conform to a metering and control application program that supports limited, largely fixed functionality**." ('193 9:67-10:9)

(Alexander Decl. Exh. D. at 24-1(Q), 24-10(G).)

**The VDE Mechanisms**: The Big Book describes various embodiments for providing these (and other) core "invention" capabilities. It describes no embodiment, however, that is said to achieve these "invention" capabilities without using at least the described VDE controls, VDE "secure containers," and VDE "secure processing environments." On the contrary, the Big Book emphasizes that the design of its VDE components is an "Important Feature" of the "invention." (See Alexander Decl. Exh. D at 24-1(S) ('193 21:43-45, 34:25-30).)

None of the above capabilities and components is merely an optional characteristic of some embodiment. They are core, defining features of the "present invention."

## IV. THE "INVENTION" PROMISES THAT IT IS ABLE TO PREVENT ALL ACCESS TO AND ALL USE OF PROTECTED CONTENT EXCEPT AS AUTHORIZED BY VDE CONTROLS

Another aspect of the VDE "invention" is particularly important to claim construction.

**Non-Circumventable**: VDE claims that the protections it promises cannot be bypassed, i.e., they are not circumventable. Rather, VDE intercepts attempts by any and all users (including would be misusers) to access or use protected information. It thereby "ensures" that the VDE controls designed to govern such access and use, in fact do so, and that all unauthorized access and use is "prevented." (See Alexander Decl. Exh. D at 24-5(A), 19(K) ("VDE enables parties ... to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled" ('193 6:18-31); "the present invention ensures that content control information can be enforced." ('193 46:4-8).) As stated at '193 11:8-11:

> "**All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used.**

This non-circumventable "access control" is critical to a proper construction of these patent claims. The secrecy of digital information (e.g., an electronic vote) may be protected by encrypting it. Encryption does not, however, provide full protection. (See Reiter Depo. at 49:7-14, 53:1-11, 55:13-16.) It does not prevent an attacker from deleting the content, or altering it, copying it, tracing it, or moving it. Thus, as the "invention" prevents all types of misuse, it does more than merely encrypt content. Specifically, VDE promises those who entrust their valuable content to it, that VDE is able to prevent all forms of unauthorized access to the content. By preventing unauthorized access, VDE prevents all unauthorized uses, including misuses which are not prevented by mere encryption (such as deleting, altering, copying, or moving the content). In other words, VDE promises a second layer of protection—a bank vault like "access control" that cannot be circumvented:

> "The virtual distribution environment 100 **prevents use** of protected information except as permitted by the "rules and controls" (control information). ('193 56:26-28)
>
> "As mentioned above, virtual distribution environment 100 'associates' content with corresponding 'rules and controls,' and **prevents the content from being used or accessed** unless a set of corresponding 'rules and controls' is available." ('193 57:18-22)
>
> "Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information **to prevent this information from ever becoming available to users even in encrypted form.**" ('193 166:59-64)

InterTrust's expert, Prof. Reiter, has agreed that the '193 Patent says that VDE is able to prevent physical access to protected content. (See Reiter Depo. at 55:17-60:1). Nevertheless, InterTrust's proposed constructions uniformly disregard this core VDE promise.

This "access control" capability of the "invention" is critical to a proper understanding of the most important claim terms in dispute. For example, various claims promise protections against unauthorized "use" or "copying" of protected content. InterTrust's proposed constructions of "use" and "copy" assume that only encryption is used to protect the content. Thus, per InterTrust, "use" and "copy" must mean only those types of uses and copying which can be prevented with encryption. That construction is wrong because that assumption is wrong. VDE promises content access control, not just encryption. In this VDE context, the claims protect against all forms of use and copying, not just those which require decryption.

## V. CLAIMS CONSTRUCTION LAW

### A. General Claim Construction Legal Analysis

The statutory measure of a patent's scope is its patented "invention," which is required to be set forth "distinctly" in the patent claims. 35 U.S.C. § 112, ¶ 2. There are statutory requirements to help ensure that what is claimed is the "invention." One is that a patent may claim as its invention only subject matter that "the applicant regards as his invention." 35 U.S.C. § 112, ¶ 2. Another is that a patent may claim only the "invention" described in the patent application's written description. 35 U.S.C. § 112, ¶ 1. These requirements, coupled with the public notice function of a patent, explain why it is fundamental that "claims are to be construed in the light of the specifications and both are to be read with a view to ascertaining the **invention**." Adams, 383 U.S. at 49; see also Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576 (Fed. Cir. 1996) ("the public is entitled to rely" on the instrinsic evidence for notice as to what the patent does and does not cover). Last year the Supreme Court confirmed this necessary link: "What is claimed by the patent application must be the same as what is disclosed in the specification." Festo, 535 U.S. at 736 .

The standard claim construction rules are set forth in Vitronics. See 90 F.3d at 1582-83 (citing Markman v. Westview Instrs., Inc., 52 F.3d 967 (Fed. Cir. 1995), aff'd, 517 U.S. 370

(1996)). See also Schering Corp. v. Amgen Inc., 222 F.3d 1347, 1353 (Fed. Cir. 2000) (interpreting patent terms as one of skill in the art at the time of the application would understand them). In ascertaining the patent's "invention," the claims' language is of primary importance. See Vitronics, 90 F.3d at 1582. However, courts must look also to both "intrinsic" and "extrinsic" evidence. See Lacks Indus. v. McKechnie Vehicle Components USA, Inc., 2003 U.S. App. LEXIS 4471, at *14 (Fed. Cir. Mar. 13, 2003) (for claim construction, "we begin with an examination of the intrinsic evidence, i.e., the claims, the other portions of the specification, and the prosecution history (if in evidence). Courts may also review extrinsic evidence in construing a claim. Additionally, dictionary definitions, although extrinsic, may be used to establish a claim term's ordinary meaning.") (internal citations omitted) (See Tab B, hereto).

Among the intrinsic evidence, "the specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." Vitronics, 90 F.3d at 1582.[4] "One purpose for examining the specification is to determine if the patentee has limited the scope of the claims." Watts v. XL Sys., Inc., 232 F.3d 877, 882 (Fed. Cir. 2000). In making this determination, however, courts must refrain from reading in unnecessary limitations from the specification into the claims. See Comark Communications, Inc. v. Harris Corp., 156 F.3d 1182, 1186 (Fed. Cir. 1998).

Recent Federal Circuit decisions have proposed that a way to help ensure this balance is to first look to the "ordinary meaning" of claim terms, then review the specification and prosecution history to ensure that it is appropriate to apply the "ordinary meaning." See Texas Digital Sys., Inc. v. Telegenix, Inc., 308 F.3d 1193, 1201-04 (Fed. Cir. 2002) (construing, *inter alia*,

---

[4] InterTrust's brief erroneously implies that a patent specification's purpose is limited to providing an enabling disclosure. (InterTrust Br. at 4:17-18). However, Federal Circuit precedent makes clear that even when the claims are plain on their face, it is necessary to consult the specification during claim construction. See Prima Tek II, L.L.C. v. Polypap, S.A.R.L., 318 F.3d 1143, 1148 (Fed. Cir. 2003) ("After identifying the plain meaning of a disputed claim term, the court examines the written description and the drawings to determine whether use of that term is consistent with the ordinary meaning of the term."); Texas Digital Sys., Inc. v. Telegenix, Inc., 308 F.3d 1193, 1204 (Fed. Cir. 2002) ("the intrinsic record also must be examined in every case").

"activating" in accordance with the ordinary meaning, consistent with the intrinsic evidence, and not accepting patentee's broader proposed construction). Under this approach, the first challenge is to determine whether there is an "ordinary meaning." Id. To do so, courts look to the plain language of the claims and determine whether **appropriate** dictionaries or treatises provide guidance as to the meaning of the terms. See id. at 1202-04; cf. Hoechst Celanese Corp. v. BP Chems. Ltd., 78 F.3d 1575, 1580 (Fed. Cir. 1996) ("a general dictionary definition is secondary to the specific meaning of a technical term as it is used and understood in a particular technical field."). Courts then "must" examine the intrinsic record to ensure consistency with the "ordinary" meaning; "[i]ndeed, the intrinsic record may show that the specification uses the words in a manner clearly inconsistent with the ordinary meaning . . . [and, in such a case, the "ordinary meaning"] must be rejected." Texas Digital, 308 F.3d at 1204. The intrinsic record may also be used to select from among various "ordinary meanings." Id. at 1203. Cf. Rexnord Corp. v. Laitram Corp., 274 F.3d 1336, 1345 (Fed. Cir. 2001) (observing that the "Summary of the Invention" section of the written description is "a pertinent place to shed light upon what the patentee has claimed.").

In certain instances, a "plain meaning" simply does not exist. See, e.g., Lacks, 2003 U.S. App. LEXIS at *16 ("the dictionary definitions do not provide a plain meaning"); J.T. Eaton & Co. v. Atlantic Paste & Glue Co., 106 F.3d 1563, 1568 (Fed. Cir. 1997) (disputed claim term "is a term with no previous meaning to those of ordinary skill in the prior art. Its meaning, then, must be found somewhere in the patent.").

Even where an ordinary meaning exists, there are several situations in which the Federal Circuit has recognized that the "ordinary meaning" is not appropriate. See, e.g., CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1366 (Fed. Cir. 2002) ("a court may constrict the ordinary meaning of a claim term in at least one of four ways"). Significant precedent establishes at least the following ways, relevant to the claims in this mini-Markman proceeding, in which claim terms should not be afforded their "ordinary meaning":

1) **To Provide Clarity**: A claim term will not have its ordinary meaning **if the term "chosen by the patentee so deprive[s] the claim of clarity" as to require resort to the other**

**intrinsic evidence for a definite meaning.**" Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1374-75 (Fed. Cir. 2003) (holding that "automation code" "is so broad as to lack significant meaning" and, thus, court limited claim to the only disclosed embodiment). See generally NeoMagic Corp. v. Trident Microsystems, Inc., 287 F.3d 1062, 1071-72 (Fed. Cir. 2002) (restricting claim to a particular type of electrical "coupling," based on specification, although dictionary definition was more general); Watts, 232 F.3d at 882-83 (holding claim term was not "clear on its face," and limiting the claim to a particular embodiment which was described as a feature of the "present invention"); Ethicon Endo-Surgery, Inc. v. U.S. Surgical Corp., 93 F.3d 1572, 1579 (Fed. Cir. 1996) (limiting "pusher assembly" to that described in drawings when the term was "ambiguous" and the specification provided "minimal guidance"); North Am. Vaccine, Inc. v. American Cyanamid Co., 7 F.3d 1571, 1576 -77 (Fed. Cir. 1993) (limiting unclear claim term "linkage to a terminal portion" to linkage at only one terminal as described in the specification).

**2) Express or Implied Definition in Patent:** "[T]he claim term will not receive its ordinary meaning if the patentee acted as his own lexicographer and **clearly set forth a definition of the disputed claim term in either the specification or prosecution history.**" CCS Fitness, 288 F.3d at 1366-67 (citing Johnson Worldwide Assoc. v. Zebco Corp., 175 F.3d 985, 990 (Fed. Cir. 1999); Rexnord Corp. v. Laitram Corp., 274 F.3d at 1342). The patent applicant's definition need not be express; when a patentee uses a claim term throughout the entire patent specification, in a manner consistent with only a single meaning, he has defined that term "by implication." Bell Atlantic Network Servs., Inc. v. Covad Communications Group, Inc., 262 F.3d 1258, 1268, 1273 (Fed. Cir. 2001) (limiting claim term "mode" to one type of mode, as the patent "defined the term 'mode' by implication" throughout the specification). See generally Abbot Labs. v. Novopharm Ltd., 2003 U.S. App. LEXIS 5357, at **13-18 (Fed. Cir. Mar. 30, 2003) (construing "a co-micronized mixture of particles of [x and y]" to mean "co-micronization of a mixture consisting essentially of only [x and y]" based on definition provided in specification) (emphasis in original) (See Tab A, hereto); Multiform Desiccants, Inc. v. Medzam, Ltd., 133 F.3d 1473,

1477-78 (Fed. Cir. 1998) (observing that an inventor may bestow "a special meaning to a term in order to convey a character or property or nuance relevant to the particular invention").

**3) Important to "Invention"**: The court will limit the ordinary meaning where the specification describes a particular feature or embodiment as "**important to the invention.**" E.g., Toro Co. v. White Consol. Indus., 199 F.3d 1295, 1301 (Fed. Cir. 1999) (limiting claim term to a unitary structure based in part on statements in the specification describing that structure as "important to the invention"). Cf. Scimed Life Sys. v. Advanced Cardiovascular Sys., 242 F.3d 1337, 1342-43 (Fed. Cir. 2001) (limiting claim term "lumen" to "coaxial lumen" in part because the specification characterized the coaxial configuration as part of the "present invention.")

**4) Distinguishing Prior Art**: "[A] claim term will not carry its ordinary meaning if the intrinsic evidence shows that the **patentee distinguished that term from prior art on the basis of a particular embodiment**," CCS Fitness, 288 F.3d at 1366-67 (citing Spectrum Int'l Inc. v. Sterilite Corp., 164 F.3d 1372, 1378 (Fed. Cir. 1998) (narrowing a claim term's ordinary meaning based on statements in intrinsic evidence that distinguished claimed invention from prior art). See generally Rheox, Inc. v. Entact, Inc., 276 F.3d 1319, 1325-26 (Fed. Cir. 2002) (restricting claim to a particular type of phosphate in light of prosecution history disclaimer of other types of phosphate, despite specification's description of some of the "disclaimed" types of phosphate); Innovad Inc. v. Microsoft Corp., 260 F.3d 1326, 1332 (Fed. Cir. 2001) (restricting claim to devices that did not have keypads, based on specification and prosecution history statements distinguishing prior art).

**5) Express Disclaimer:** A claim term will not carry its ordinary meaning if the intrinsic evidence shows the patentee **"expressly disclaimed subject matter."** CCS Fitness, 288 F.3d at 1366-67. See generally Scimed, 242 F.3d at 1342-44 (limiting claim term based in part on statements in the specification indicating the invention "excludes" other structures); Ballard Med. Prods. v. Allegiance Healthcare Corp., 268 F.3d 1352, 1361-62 (Fed. Cir. 2001) (finding an explicit disclaimer of "pressure valves" and "dynamic seals" where patentee asserted that his invention, in contrast to such prior art, comprised "vacuum valves" and "static seals").

As shown above, District Courts, the Federal Circuit, and the Supreme Court frequently determine the scope of the "invention" described in the patent specification in the course of determining scope of the issued claims. Where there is a possible disconnect between the disclosed "invention" and the claims, the Federal Circuit normally will construe the claims narrowly, rather than invalidate the claims. See, e.g., Tate Access Floors, Inc. v. Interface Architectural Res., Inc., 279 F.3d 1357, 1367 (Fed. Cir. 2002) ("claim language should generally be construed to preserve validity, if possible"); Schering Corp., 222 F.3d at 1353-54 (limiting claim to one subspecies, as that was all that was described and enabled by specification). However, where the claim on its face is clear and there is no link or "hook" at all in the claim for what the patent described as the "invention," then the Court may construe the claim broadly, but invalidate it under Sec. 112, ¶ 2 or ¶ 1. See, e.g., Cardiac Pacemakers, Inc. v. St. Jude Med., Inc., 296 F.3d 1106, 1114 (Fed. Cir. 2002) ("where the specification fails to disclose structure corresponding to the claimed function, [preserving validity] is impossible [so] the claims are invalid."); Tate Access, 279 F.3d at 1372 ("where claim language is clear we must accord it full breadth even if the result is a claim that is clearly invalid.").

**B. Other Claim Construction Issues In This Case**

**1. Incorporation f One Pending Application Into Another By Reference**

Three InterTrust patents (the '683, '721, and '861) purport to incorporate the Big Book by reference to the unpublished patent **application**. (See '721 at 1:7-19; '683 at 1:11-23; '861 at 1:7-11.) However, the specifications of these three patents were never amended to properly reference the Big Book's issued patent number, as required by the Patent Office. See In re De Seversky, 474 F.2d 671 (C.C.P.A. 1973); Manual of Patent Examining Procedure § 608.01(p). This failure means that the Big Book is not part of the "specifications" of these three patents. Nonetheless, the Big Book remains intrinsic evidence for the '683 Patent (as it is in that patent's prosecution history) and extrinsic evidence for the others.

**2. Restriction Requirements and Divisional Patent Applications**

InterTrust argues that a Patent Office restriction requirement "conclusively rebuts"

Microsoft's position that the Big Book is drawn to a comprehensive VDE "invention." InterTrust's argument misses the mark for several reasons.

First, the claim construction point being made by Microsoft is that all of these claims necessarily invoke the required "features" of the VDE "invention," not that all claims require only those features. InterTrust's patent claims are free to recite additional features, which additional limitations may (or may not) make them separate "inventions" under Patent Office restriction practice. But, that is not the issue here.

Moreover, in entering the restriction requirement, the Patent Office did not indicate that it was construing the claims as non-VDE claims, requiring none of the required features of the disclosed "invention." Rather, the Patent Office merely grouped the original claims of the "Big Book" application into different categories that were supposedly "related as subcombinations disclosed as usable together in a single combination." (InterTrust Brief at 11 (citing September 25, 1996, Office Action at 2-3.) InterTrust admits in its opening brief that Rambus Inc. v. Infineon Techs., 318 F.3d 1081 (Fed. Cir. 2003), is distinguishable because none of the restriction requirements here specifically involved the VDE limitations, whereas in Rambus the limitation at issue was directly involved in the restriction requirement. (InterTrust Br. at 13, n. 7).

Also, that a restriction requirement was made does not mean that subsequent claims are directed to separate inventions. Rather, a court must closely scrutinize the scope of claims issuing from a divisional application. Gerber Garment Tech., Inc. v. Lectra Sys., 916 F.2d 683, 688 (Fed. Cir. 1990) (invalidating divisional claims for double patenting, because applicant had amended such that they were no longer distinct inventions). Here, as in Gerber, the claims at issue were changed from the original application claims that "spun off" after the restriction requirement. (Alexander Decl., ¶¶ 17.) Consequently, any "presumption" that these issued claims are directed to a different "invention" should not apply.

Finally, courts have limited claims based on descriptions in the specification, despite the fact that a patent issued from a "divisional" application. See Ballard, 268 F.3d at 1360-62 (Fed. Cir. 2001) (limiting claims of both a patent issued from the parent application and a patent issued

from a divisional of such parent to exclude a particular type of valve based on statements made in common specification text and prosecution history of the parent application).

**3. Claim Terms Are Construed Consistently in Related Patents**

InterTrust incorrectly asserts that "divisional" patents should be separated from their parent. On the contrary, related patents should be construed consistently. Specifically, terms in patent families should generally be afforded the same construction. See AbTox, Inc. v. Exitron Corp., 131 F. 3d 1009, 1001 (Fed. Cir. 1997), amending on reh'g 122 F.3d 1019 (Fed. Cir. 1997) ("Although these claims have since issued in separate patents, it would be improper to construe this term differently in one patent than another, given their common ancestry.") Also, limitations set forth in one patent's specification or prosecution history, may act as a limitation on the related patents. Elkay Mfg. Co. v. Ebco Mfg. Co., 192 F.3d 973, 980 (Fed. Cir. 1999) ("When multiple patents derive from the same initial application, the prosecution history regarding a claim limitation in any patent that has issued applies with equal force to subsequently issued patents that contain the same claim limitation"); see also Mark I Mktg. Corp. v. R.R. Donnelley & Sons Co., 66 F.3d 285, 291 (Fed. Cir. 1995) (restricting claim scope based on prosecution of "grandparent" application).

## VI. EACH OF THE TWELVE CLAIMS SHOULD BE CONSTRUED TO REQUIRE THE DISCLOSED "INVENTION"

### A. '193, Claims 1, 11, 15, 19

The '193 Patent publishes the Big Book specification without any substantive additions (and thus is cited throughout this Brief as a surrogate for the Big Book).

Contrary to InterTrust's position (InterTrust Br. at 8:9-10), all four '193 Patent mini-Markman claims concern the distribution and protection of digital content, and contemplate multiple nodes and participants. Information is received (possibly from multiple upstream content providers), then stored on a device having unspecified authorized and unauthorized users, and then conditionally transferred to another device having unspecified users. The claims promise to control three forms of unauthorized use of this distributed content: copying, distributing (to the second device), and storing (on the first and/or second device):

"if said copy control allows at least a portion of said digital file to be copied and stored on a second device...." ('193 321:10-11)

"determining" or "determine" "whether said digital file may be copied and stored on a second device ...." ('193 321:7-9)

This claim language (e.g., "if ... allows," "determining whether") is not qualified. It implies that if the copying and storing are not allowed, then they are prevented (see Reiter Depo. at 174:1-178:11), no matter what effort may be made to take the unauthorized action. In other words, these claims imply that their "controls" are effective in the face of the attacks identified in the Big Book.

These claimed protections against misuse cannot be achieved by encrypting the content. Encryption would not prevent the content from being accessed, copied, distributed, or stored. For these types of protection, "access control" is necessary. More particularly, the Big Book describes only the complete "invention" as providing such protection against the threats identified in the Big Book. In other words, by promising the type of effective access control protection said to be provided only by the complete VDE, these claims invoke that "invention." Their use of the vague, VDE term "control" also invokes the "invention."

**B. '683, Claim 2**

The '683 Patent is a "continuation-in-part" (CIP) which does not contain the Big Book's text. Although it purports to incorporate the Big Book, it fails the Patent Office's rules for incorporating "essential matter." (See supra, V. B.1 at 14.) Nevertheless, the Big Book is part of this patent's prosecution history, and thus is intrinsic evidence for claim construction purposes.

This claim also concerns a multi-node distribution system. Here, "secure containers" and "secure container rules" are distributed amongst various nodes. The claim appears to promise the ability to prevent access to or use of protected information, using the secure containers, secure container rules, and a "protected processing environment." (See Second Mitchell Decl. at 6-7.) These protections are not qualified as to the nature or severity of the threat being faced; they impliedly are effective against all threats identified in the patent or Big Book. The only system described in the Big Book or '683 Patent said to accomplish such protections, is the complete

VDE. This claim further invokes VDE by using VDE and vague terminology, such as "secure container" and "protected processing environment."

**C. '721, Claims 1, 34**

The '721 Patent neither contains the Big Book, nor incorporates it in the manner required by the Patent Office for incorporating essential matter into a patent. Moreover, the Big Book is not in the '721 Patent's Patent Office prosecution history. Thus, the Big Book is merely extrinsic evidence for purposes of construing these claims.

The '721 Patent purports to improve the Big Book VDE by preventing the use of executable code (specifically, "load modules" in Claim 1) except as authorized. Such prevention requires an access control capability. Claims 1 and 34 promise such protections without any qualification that they are effective only sometimes, or in some situations. Neither the Big Book nor the '721 Patent describes anything other than a full VDE system for achieving these types of promised results in the face of the threats identified in those documents. These claims further invoke the "invention" by reciting several terms that invoke VDE for context, including "protected processing environment," "tamper resistant barrier," and "security."

**D. '861, Claim 58**

The Big Book also is merely extrinsic evidence for purposes of construing this claim.

This patent discusses a possible attack on the "security" of "secure containers." It requires that the process of creating VDE secure containers be itself protected. ('861 4:51-64)

Claim 58 recites such a method for creating secure containers. It appears to promise the ability to prevent any access to or use of certain information (by putting the information in a secure container), except as authorized by a rule. It also provides a particular rule designed to control at least one aspect of allowed use or access. Again, the promised protection is not qualified by type or severity of threat. Neither this patent nor the Big Book describes any non-VDE system for achieving this promised capability. This claim further invokes VDE by reciting various vague and VDE terms, including "secure container" and "control."

**E. '891, Claim 1**

This patent publishes the Big Book without addition.

This claim appears to make the unqualified promise that it prevents an appliance from using content protected by controls received from two remote entities, except as authorized by those controls. This ability to prevent all use implies an ability to control access. Again, the patents describe no non-VDE system having this capability. This claim also uses several vague and VDE terms, such as "secure operating environment," "securely receiving," "control," "securely processing," and "securely applying."

**F. '900, Claim 155**

This patent repeats the Big Book, but also adds to it. It addresses various possible attacks against VDE's protections, including one in which a VDE's foundation software (which, e.g., runs to create a VDE "host processing environment") is copied onto another machine to form a rogue VDE node. ('900 233:8-15). One of the solutions described in this patent is to embed a unique identifier, called a "machine signature," into the VDE software so that it cannot run on a different machine. ('900 237:40-54, 239:5-14).

Claim 155 recites a method using "machine check programming" for checking a VDE host processing environment and halting processing. This method also is unqualified, i.e., it does not rule out any of the types or severities of threat described in this patent. Also, it uses several VDE specific or otherwise vague terms, such as "virtual distribution environment," "host processing environment," "machine check programming," and "tamper resistant software," which need to be clarified and construed in light of the VDE "invention."

**G. '912, Claims 8, 35**

This patent is a "divisional" patent which publishes the Big Book without change.

These claims are somewhat similar to those of the '721 Patent. Claim 8 appears to promise the ability to prevent use of a load module within an execution space, except as authorized. Claim 35 appears to promise the unqualified ability to prevent use of certain "specified information," in part by protecting the process of creating the "component assembly" which controls that use. By preventing unauthorized uses, each claim implies an access control capability. Again, the Big Book describes no non-VDE system with this unqualified capability. These claims also use several VDE or vague terms, such as "component assembly," "load

module," "level of security," "securely assembling," and "secure container."

In sum, had these twelve claims used only precise, well-defined, non-VDE terminology, and not promised the types and levels of protection provided by VDE, then they might not have invoked the disclosed "invention." That, however, is not the case.

## VII. CONSTRUCTION OF THE CLAIM TERM "USE"

**Central Dispute**: Whether an encrypted file may be "used" without decrypting it.

As explained above, VDE prevents all forms of unauthorized "use" of protected information, including forms of misuse which do not require decryption, such as deleting or altering someone else's encrypted content.

**Ordinary Meaning**: Microsoft's construction follows from the ordinary, everyday meaning of "use." A "use," of course, may be a "misuse." In "security" systems, the most important uses to address are the potential misuses, including those by unauthorized users. Microsoft's construction does that, and includes several uses which may be misuses (such as deleting someone else's data).

**Microsoft's Construction**: "(1) To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.)...." (JCCS Exh. A at Row 42).

This is precisely how the term "use" is used in the Big Book and '683 Patent:

> "These appliances typically include a secure subsystem that can enable control of **content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage**, etc." ('193 9:24-27)
>
> "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that **the moving, accessing, modifying, or otherwise using of information** can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-31)
>
> "Provides non-repudiation of use and may record specific **forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.**" ('683 6:46-48)

(Alexander Dec. Exh. D at 23(G), 23(C), 23(A).) Nothing in these patents counters these Big

Book definitions of "use" as including copying, encrypting, saving, modifying, and moving.

Importantly, many of these actions which the Big Book refers to as "uses" cannot be blocked by encryption and, conversely, require no decryption of the content to perform. That such uses are indeed "uses," is further confirmed by the parties' agreed definition of "tampering" (which includes "altering" within "use" (see JCCS Exh. I at Row 8)), and InterTrust's proposed definition of "VDE" (which includes "distribution" within "use" (see JCCS Exh. A at Row 86)).

Microsoft's proposed construction further requires that "(2) In VDE, information Use is Allowed only through execution of the applicable VDE Control(s) and satisfaction of all requirements imposed by such execution." (See JCCS Exh. A at Row 42). This is VDE's "prevent unauthorized use" protection mechanism, governed by VDE controls, which is found throughout the Big Book, and explained by Prof. Maier (Maier Decl. at 7-8, 38-41).

**InterTrust's Proposed Construction**: InterTrust's proposed construction of "use" is typical of most of its constructions: short, unclear, and contrary to the Big Book: "to put into service or apply for a purpose, to employ." (See JCCS Exh. A at Row 42). This loose language may be fine as a general concept, but is not adequate for a claim construction. It does not clearly or precisely define the types of use (e.g., misuses) of digital information it encompasses or excludes. On the contrary, it would leave the jury and public guessing about which of the following actions, **expressly identified as "uses" in the patents**, are "uses": copying, encrypting, saving, modifying, and moving.

InterTrust apparently contends that nothing is a "use" of information if it cannot be prevented by encryption alone. In other words, if content is encrypted, a "use" of that information must require decryption, or else it is not a "use." Per InterTrust, apparently, none of these Big Book uses, is a use: deleting content, altering it, saving it, encrypting it, copying it, or moving it.

This position is contrary to the Big Book's above-quoted express statements that "use" includes deleting, saving, encrypting, moving, and copying. More importantly, it is contrary to the core promise of the VDE "present invention" that its access control capabilities can prevent all unauthorized access to and use of protected content, not just those uses which could be

blocked through encryption.

The Court should expressly include within "use" all of those actions expressly identified as "uses" in the Big Book and the '683 Patent, as set forth in Microsoft's construction.

## VIII. CONSTRUCTION OF THE CLAIM TERM "COPY"

**Central Dispute**: Whether a reproduction is still a "copy" if it is unusable or inaccessible to someone.

**Ordinary Meaning**: Under its ordinary meaning, to "copy" something is to reproduce it, and the resulting reproduction is a "copy." The copy, of course, remains a copy even if it is locked away and inaccessible. It also remains a copy if given to someone who cannot use it.

**Microsoft's Construction**: "(1) To reproduce all of a Digital File or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. (2) Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. (3) **The resulting "copy" may or may not be encrypted, ephemeral, usable, or accessible.**" (See JCCS Exh. A at Row 5).

This is how the Big Book uses the term "copy." A copy of an encrypted electronic file is still a copy even when possessed by someone who has no right to decrypt it or otherwise use it. Thus, the Big Book refers to a reproduction of a video program as a "copy" even though its recipient cannot watch or copy it: "Even if a consumer has a **copy of a video program**, she cannot watch or copy the program unless she has "rules and controls" that authorize use of the program." ('193 53:60-62). On the other hand, when the Big Book means a copy which is usable, it says so: "For example, if a software program was distributed as a traveling object, a user of the program who wished to supply it or a **usable copy** of it to a friend would normally be free to do so." ('193 131:65-132:1). (Alexander Dec. Exh D at 10(C)-10(E).)

InterTrust's expert, Prof. Reiter, has testified that this everyday "reproduction" sense of the word "copy," in which a copy is still a copy even if possessed by someone who cannot

decrypt it, is "a very common use of the word 'copy.'" (Reiter Depo. at 64:12-65:8, 66:1-15)). He also has conceded that the Big Book used the term "copy" in this manner in the above "video program" quote, and elsewhere. (Reiter Depo. at 68:5-70:7, 74:21-75:17).

**InterTrust's Proposal**: Despite this usage in the Big Book and these concessions of its expert, InterTrust nevertheless urges the Court to dismiss this "very common" usage and construe "copy" as if a copy is no longer a copy when locked away or given to someone who cannot decrypt it. Rather than expressly say so, however, InterTrust says merely that "the reproduction must be useable." (See JCCS Exh. A at Row 5). As interpreted by its expert, Prof. Reiter, InterTrust does not here mean "usable" in the VDE sense of "use" (described above). Rather, by "must be usable," InterTrust apparently means that a reproduction of encrypted content is not a copy when possessed by someone who cannot decrypt it. In other words, whereas the '193 claims expressly limit the number of "copies" which can be made, InterTrust urges the Court to read these claims as if they limit the number of "decryptable (by present holder) copies." InterTrust's proposal is unworkable, contrary to the specification's use of "copy," and wholly divorced from the core VDE "prevent unauthorized access" capability.

Unworkable: Under InterTrust's apparent theory, a non-copy would become a copy when handed to someone who can decrypt it, and then become a non-copy again when handed back. Such a vacillating status as "copy" is not workable. How can a system "control copying," if the reproduction's status as a "copy" depends on who happens to possess it in the future?

Contrary to Specification: The Big Book not once suggests that a "copy" **must** be decryptable or "usable." On the contrary, as noted above, the Big Book focuses on ways to **prevent** use (e.g., misuse) of files and copies; expressly states that one needs appropriate controls to use a "copy" ('193 53:60-63); and refers to a "usable copy" to indicate that controls allow the copy to be used ('193 131:67). Indeed, Prof. Reiter agreed that InterTrust's proposed construction of "copy" was inconsistent with the above-quoted Big Book's use of the term "copy" in connection with a video program. (Reiter Depo. at 71:19-73:17).

Contrary to the VDE "No Unauthorized Access" Promise: Perhaps most importantly, in its construction of "copy," InterTrust again ignores and contradicts the VDE "present invention."

These claims concern copying not only by authorized end-users, but also by unauthorized mis-users. Preventing such unauthorized copying, even by someone who is unable to decrypt those copies, is an important "security" feature. For example, unauthorized copying of encrypted files can be used as a "denial of service attack" on a computer system by replicating the encrypted files into a computer's memory to deny legitimate access to that memory by authorized users. (This attack is especially effective if the files are written to a write-only medium.) Or, an attacker could copy multiple encrypted files to his own computer to study the encryption scheme. In neither of these examples was the attacker authorized to decrypt the encrypted "copy," but he nevertheless was able to use copying of encrypted files for his own unauthorized purposes. (See Second Mitchell Decl. at 6-7 (discussing "copy").)

The claimed methods can block all unauthorized copying because VDE supposedly is able to block all access to the encrypted content. InterTrust's position wrongly assumes that only the ability to decrypt content is being controlled. In other words, by arguing that a "copy" is not usable if it cannot be decrypted (and thus is not a copy), InterTrust is trying to transform this claim which prevents all unauthorized copying (i.e., has at least two levels of protection), into a claim which merely prevents unauthorized decryption of copies (i.e., has only one level of protection).

Other Disputes Over This Term: One, of course, may copy all of something or only a portion. InterTrust argues that copying a portion of a file can be referred to as copying the file, while Microsoft submits that copying a portion is just that, copying a portion. If a claim speaks of copying a file, it means copying the entire file. When the claims, and patents, mean to refer to a portion, they say "portion." (Compare '193, Claim 1 ("copying at least a portion of said digital file"), with '193 Claim 11 ("determining whether said digital file may be copied."))

InterTrust also argues that "copying" includes altering something, "as long as the essential nature of the content remains unchanged." (See JCCS Exh. A at Row 5). That is unsupported by the patents, and unworkably vague.

## IX. CONSTRUCTION OF "SECURE"; "SECURELY"

**Central Dispute**: Whether a "secure" condition is one in which the threats identified in the patents are prevented, rather than one in which, e.g., some form of attack is detected (but not prevented).

**Ordinary Meaning**: It is well recognized in computer science that "secure" is a label for an achieved condition or state of being:

> "**State achieved** by hardware, software or data **as a result of successful efforts** to prevent damage, theft or corruption," (Spencer, 156; see Reiter Depo.at 221:4-7) (cited by InterTrust for another term)
>
> "Security is a negative attribute. **We judge a system to be secure if we have not been able to design a method of misusing it** which gives some advantage to the attacker." (Davies, p. 4)
>
> "Definition 4-1. A *security policy* is a statement that partitions the states of the system into a set of *authorized*, or *secure*, states and a set of *unauthorized*, or *nonsecure*, states . . . Definition 4-2 **A *secure system* is a system that starts in an authorized state and cannot enter an unauthorized state.**" (Italics in original) (Bishop, p. 95)

(Alexander Dec. Exh. D at 19(JJ), 19(XX), 19(TT).) (See also Reiter Depo. at 30:11-34:5, 35:9-36:18, 222:11-223:1.)

As explained in Prof. Mitchell's first Declaration, there are myriad flavors and degrees of being "secure," depending on a host of contextual variables, such as what is being protected, against what, for how long, to what degree, etc. The patents confirm this by using "secure" to mean different things in different places. The unanswerable question is what does "secure" mean in these context-light claims? (See Microsoft's Motion for Summary Judgment on Indefiniteness).

**InterTrust's Proposed Construction**: InterTrust's proposed construction of "secure" is so extreme that we address it first: "One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that Access to

information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose." (See JCCS Exh. A at Row 3).

"One or more mechanisms are employed ....": InterTrust's construction is contrary to the ordinary meaning of "secure" in many respects. First, being "secure" is like being "intelligent" or "beautiful;" it is a condition or a state of being. It is not a statement that some effort was made to become secure (or intelligent or beautiful); it is a label confirming a successful result. For example, placing a combination lock on a safe "employs" a security "mechanism," but that does not mean that the safe is "secure" (e.g., the combination might be easy to guess, or even posted on the safe; the safe's door might be left unlocked, or the safe's walls might easily be broken, etc.).

InterTrust's proposed construction is wrong in this very basic respect. It says that something is "secure" if some effort is made: the result doesn't matter. That is illogical, contrary to the ordinary meaning, and contrary to the Big Book's promises that VDE's security mechanisms can achieve a truly secure environment.

"To prevent, detect, or discourage ....": This is another example of how far InterTrust is willing to distance the claims from the VDE "present invention." Whereas the VDE invention promises the ability to **prevent** all access, use, observation, and interference with protected content, InterTrust would have the Court rule that something is "secure" even if its content is easily destroyed, copied, distributed, and read by others, so long as the system "detects" or "discourages" this misuse. Detecting misuse can be an important function that helps achieve a secure condition, but detecting alone, without preventing misuse, is not security.

Indeed, that InterTrust would urge that a "secure" container, environment, space, memory, etc., may not prevent (or even discourage) any threat whatsoever, no matter how weak the attack, illustrates how flawed its whole approach to claim construction has been. Claim construction is not a word game where one hunts for bits and pieces of definitions from dictionaries written without the "invention" in mind, and tries to fit them together to get the broadest and vaguest possible meaning of a claim term. Rather, as the Patent Statutes require, the Supreme Court has held, and the Federal Circuit has recognized, "what is claimed by the patent application must be the same as what is disclosed in the specification."

"Such mechanisms may include concealment, Tamper Resistance, Authentication and access control.": Prof. Reiter has testified that, under InterTrust's proposal, the term "secure" **does not require any** of these listed forms of protection. (Reiter Depo. at 201:14-204:14). This, again, is at odds with the Big Book's promise that VDE prevents all unauthorized access, use, observation, and interference.

"Security is not absolute, but is designed to be sufficient for a particular purpose": This statement points out a basic problem with the use of "secure" in these claims and with InterTrust's proposed construction. As with "intelligence," being "secure" is a multi-dimensional, subjective characteristic for which some objective criteria is necessary if skilled evaluators are to objectively determine whether or not something is "secure." That the term "secure" is used in the specification to refer to different things in different contexts, as InterTrust notes, only confirms why context is all important to an understanding of what the term means in the claims. Neither these claims, nor InterTrust's "sufficient for a particular purpose" proposal, however, provides such context or any objective criteria for evaluating what is or is not "secure."

The "designed to be" language of InterTrust's proposed definition language hints that, in InterTrust's view, the "purpose" necessary for evaluating whether something is secure can be gleaned not from the patents, but from the "designer" of an individual accused system or components. That makes no sense. Assume that A and B design two identical systems, each with a different "purpose" in their designs. C acquires these identical systems and offers them to a potential customer D who first wants to know whether these two identical systems are "secure" as meant in these patent claims. It simply cannot be true that one system is "secure" while the other identical system is not (because of the different purposes of their designers). Rather, the necessary context, purpose, and objective criteria for evaluating whether any given system is "secure" as meant by these claims (if it can be discerned at all), must be fixed within the patents themselves.

**Microsoft's Construction**: Unlike InterTrust's proposal, Microsoft's construction of "secure" is workable, precise, and honors the basic premise of VDE. Specifically, to the extent a construction is forced onto this indefinite claim term, it should be that the term "secure" indicates

that each type of property identified in the patents is "truly secure" against all types and levels of threats identified in the patents. In part, this means that "secure" is "(1) A state in which all users of a system are guaranteed that all information, processes, and devices within the system, shall have their availability, secrecy, integrity, authenticity and nonrepudiation maintained against all of the identified threats thereto." (See JCCS Exh. A at Row 3).

This is not a standard definition of "secure." Nor is it an express definition from the Big Book (which doesn't offer one). But, if the Court denies Microsoft's indefiniteness motion, and finds the term "secure" sufficiently clear to construe, this is the fairest approach to that construction. Specifically, this "true security" construction follows from InterTrust's assertion that "security is designed to be sufficient for a particular purpose." Here, the Big Book describes a wide range of possible security threats, including strong and sophisticated attacks against valuable information where only this proposed "true security" would be acceptable. None of the patent claims excludes such high-value, strong-attack situations. On the contrary, they apparently maintain a secure state in the face of all attacks mentioned in the patents. Therefore, the fairest construction is the one that makes sense over the whole range of disclosed attack situations, namely "true security" where all properties are protected against all attacks identified in the Big Book.

## X. CONSTRUCTION OF "SECURE CONTAINER"

**Central Dispute**: Whether a "secure container" must prevent unauthorized access to its contents.

A VDE secure container is one of the core VDE components that provide the capabilities touted in the Summary of the Invention.

**Ordinary Meaning**: The parties agree that the term "secure container" has no ordinary meaning in this field. (See, e.g., Reiter Depo. at 275:6-276:10.)

**Microsoft's Construction**: (1) A VDE Secure Container is a self-contained, self-protecting data structure which ... (b) cryptographically protects that information from all unauthorized Access and Use, ... (d) permits the association of itself or its contents with Controls

and control information governing (Controlling) Access to and Use thereof, and (e) prevents such Use or Access (as opposed to merely preventing decryption) until it is "opened." (See JCCS Exh. A at Row 57).

As used in the Big Book, a VDE "secure container" protects content it contains by preventing all access to and use of that content except as authorized by VDE via satisfactory execution of VDE controls associated with the secure container. In effect, a VDE secure container hides the content from users while VDE "controls" act as guards that escort authorized users to that content and supervise their use of it. (Alexander Dec. Exh. D at 20(A)-20(C), 20(E)-20(G).)

The Big Book describes details of only one embodiment of a secure container. In that embodiment, the secure container (in conjunction with the rest of VDE) blocks all direct access to its contents, and requires satisfaction of several controls, including one created by an ACCESS method[5]:

> "Even if the object is stored locally to the VDE node, **it may be stored as a secure or protected object[6] so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object.**" ('193 192:14-19)

A secure container, then, is part of the second layer of protection discussed above. As noted in the below quote, not only is the content "encrypted" (first layer of protection) but so is the "content source and routing information" (second layer).

> "ACCESS method 2000 reads the ACCESS method MDE from the secure database, reads it in accordance with the ACCESS method DTD, and **loads encrypted content source and routing information** based on the MDE (blocks 2010, 2012). **This source and routing information specifies the location of the encrypted content.** ACCESS method 2000 then determines whether a connection to the content is available (decision block 2014). ('193 192:36-52)

---

[5] InterTrust construes "access" as meaning "To obtain something so it can be used," which is true, although incomplete.

[6] This sentence refers to a "secure object." In VDE, a "container" and its contents "can be called an 'object.'" ('193 58:43-44).

Prof. Maier explains this VDE "secure container" mechanism at greater length. (See also Reiter Depo. at 117:18-23; 125:20-126:4; '683 Patent 15:67-16:4. Maier Decl. at 38-41.)

This "access control" ability of VDE secure containers is critical to VDE's promise to content owners that it can prevent (not simply detect) all access to and use (not just decryption-based uses) of protected content. Without this access control ability of VDE generally, and secure containers in particular, VDE's promised ability to control, govern, audit, etc. all accesses and uses, would be a lie.

**InterTrust's Proposed Construction**: InterTrust's proposed construction of "secure container" is a far cry from the VDE "secure container": "A Container that is Secure." (See JCCS Exh. A at Row 57). As this is interpreted by Prof. Reiter, merely detecting a single form of misuse of some of its contents, would make a container a "secure container," even if the container could not prevent **any** unwanted access, misuse or interference with the contents. That certainly does not sound "secure," and, more importantly, makes no sense in light of the Big Book's and other InterTrust patents' proclamations of the abilities of a VDE secure container:

> **"Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility."** ('683 8:50-52).
>
> "Even if the object is stored locally to the VDE node, **it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object.** ('193 188:59-67).

## XI. CONSTRUCTION OF "TAMPER RESISTANT BARRIER"

| |
|---|
| **Central Dispute**: Whether a "tamper resistant barrier" must be a physical device, and prevent unauthorized access, observation, and interference. |

Another of the required VDE mechanisms for providing the promised VDE capabilities, is a VDE secure processing environment, formed by a hardware-based tamper resistant barrier.

**Ordinary Meaning**: The ordinary meaning of "tamper resistant barrier" denotes a physical device. More specifically, the term "tamper resistant barrier" would have been understood in 1995 in reference to cryptographic coprocessors such as smart cards. (See Reiter Depo. at 137:15 – 138:17).

**Microsoft Construction**: "(1) An active device that encapsulates and separates a Protected Processing Environment from the rest of the world. (2) It prevents information and processes within the Protected Processing Environment from being observed, interfered with, and leaving except under appropriate conditions ensuring security. (3) It also Controls external access to the encapsulated Secure resources, processes and information. (4) A Tamper Resistant Barrier is capable of destroying protected information in response to Tampering attempts." (See JCCS Exh. A at Row 71).

To properly construe this term requires consideration of another "access control" promise of VDE.

As noted above, VDE concerns both security **and** commerce. Hence, it does not just prevent unauthorized access to protected content, it also allows and governs authorized access to, and use of, that content. That, however, presents a possible security hole. The processes used to allow and govern authorized access or use might be observed by attackers and altered to permit improper access to and use of protected content. Therefore, as a corollary to its promise to prevent protected **content** from any unauthorized access, VDE also promises that it is capable of preventing (not merely detecting) all unauthorized observation of and interference with the VDE **processes** which govern such access and use.[7]

> "SPU 500 is enclosed within and protected by a '**tamper resistant security barrier' 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions.**" ('193 59:48-53)
>
> "SPU 500 provides a tamper-resistant protected processing environment ("PPE") in which processes and transactions can take place securely and in a trusted fashion." ('683 16:60-62)

Prof. Reiter has agreed that the Big Book describes mechanisms to prevent all types of tampering (unauthorized interference) with VDE processes. (Reiter Depo. at 55:17-60:1).

---

[7] Whether users can choose not to use all of a system's capabilities does not change the fact that those capabilities allegedly exist.

This corollary promise—the ability to prevent VDE processes from unauthorized observation and interference—informs the proper construction of "tamper resistant barrier." As described in the first above quote, a tamper resistant barrier encapsulates a special-purpose "Secure Processing Unit" (SPU). This physical tamper resistant barrier prevents both information and processes within the Protected Processing Environment from being "observed, interfered with, and leaving" except under appropriate conditions ensuring security.

> "SPU 500 in this example is an integrated circuit ("IC") "chip" 504 including "hardware" 506 and "firmware" 508. ... "Hardware" 506 also contains long-term and short-term memories to store information securely so **it can't be tampered with.**" ('193 59:60-60:3)

> "BIU 530 is **designed to prevent unauthorized access to internal components within SPU 500 and their contents.** It does this by only allowing signals associated with an SPU 500 to be processed by control programs running on microprocessor 520 and not supporting direct access to the internal elements of an SPU 500." ('193 69:6-11)

As InterTrust notes, the Big Book also refers to a "tamper resistant barrier" which is not a physical, hardware device. However, the "tamper resistant barrier" in the mini-Markman claims is properly construed as the hardware variant, for three reasons.

First, the Big Book promises "true" security. It promises the ability to "prevent" unauthorized uses, etc., and "ensure" that rights will be enforced, and "guarantee" trustworthiness, even when faced with strong, sophisticated attacks against high-value content. Nothing in the claims indicates an inability to live up to these promises and protect such high-value content against such strong attacks. Only the hardware-based tamper resistant barrier is described as providing that sort of true protection for the most valuable content in even high-risk surroundings.

> "HPEs 655 may (as shown in FIG. 10) be provided with a software- based tamper resistant barrier 674 that makes them more secure. Such a software-based tamper resistant barrier 674 may be created by software executing on general-purpose CPU 654. Such a 'secure' HPE 655 can be used by ROS 602 to execute processes that, while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. **The SPU 502 may be used to perform all truly secure processing, whereas one or more HPEs 655 may be used to provide additional secure (albeit possibly less secure than the SPE) processing** using host processor or other general purpose resources that may be available within an

electronic appliance 600. Any service may be provided by such a secure HPE 655" ('193 80:22-36)

> **"No software-only tamper resistant barrier 674 can be wholly effective against all of these threats. A sufficiently powerful dynamic analysis (such as one employing an in-circuit emulator) can lay bare all of the software-based PPE 650's secrets.** Nonetheless, various techniques described below in connection with FIG. 69A and following make such an analysis extremely frustrating and time consuming--increasing the 'work factor' to a point where it may become commercially unfeasible to attempt to 'crack' a software-based tamper resistant barrier 674." ('900 233:24-33)

Second, if these claim terms were construed to cover the software variants, they would be much too vague. There would be no objective measure for distinguishing between a barrier which is tamper resistant and one which is not tamper resistant.

Third, the Big Book states that a Secure Processing Unit (with its physical tamper resistant barrier) is **necessary** wherever protected content is assigned usage related control information, or used. As all of the mini-Markman claims contemplate one or both of these two conditions, each claim necessarily requires a hardware tamper resistant barrier.

> "VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. **VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a 'virtual black box,' a collection of distributed, very secure VDE related hardware instances** that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means." ('193 15:14-27)

> **"Summary of Some Important Features Provided by VDE in Accordance With the Present Invention** ... VDE employs **special purpose hardware** distributed throughout **some or all locations** of a VDE implementation: a) **said hardware controlling important elements of**: content preparation (such as causing such content to be placed in a VDE content container and associating content control information with said content), content **and/or** electronic appliance usage auditing, content usage analysis, **as well as content usage control**; and b) said hardware having been designed to securely handle processing load module control activities, wherein said control processing activities may involve a sequence of required control factors" ('193 21:43-45; 22:20-31)

> **"A hardware SPU (rather than a software emulation) within a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required.** ('193 49:15-17)

> "**Physical facility and user identity authentication security procedures** may be used **instead of hardware SPUs** at **certain nodes**, such as at an established financial clearinghouse, **where such procedures may provide sufficient security** for trusted interoperability with a VDE arrangement employing hardware SPUs at user nodes." ('193 45:60-65)

(See also Maier Decl. at 9-11.)

**InterTrust's Proposed Construction**: "Hardware and/or software that provides Tamper Resistance." InterTrust defines "Tamper Resistance" as "Making tampering more difficult and/or allowing detection of tampering." (See JCCS Exh. A at Row 67).

This proposal raises more questions than it answers. For example, "making tampering more difficult" than what? What does "allowing detection of tampering" mean? Not preventing detection? Are the walls of straw house a tamper resistant barrier because they allow detection of a fire? And, as usual, InterTrust's proposed construction is contrary to VDE. The "invention" did not settle for mere detection; it was touted as preventing all unauthorized access, use, observation, and interference. InterTrust may regret those promises but it cannot erase them.

## XII. CONSTRUCTION OF "PROTECTED PROCESSING ENVIRONMENT"

**Central Dispute**: Whether a "protected processing environment" must have a physical "tamper resistant barrier" and prevent unauthorized access, observation, and interference.

This claim term presents the same key issue as "tamper resistant barrier."

**Ordinary Meaning**: The parties agree that there is no ordinary meaning of "protected processing environment."

**Microsoft Construction**: "(1) A uniquely identifiable, self-contained computing base trusted by all VDE nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the February, 1995, patent application as being protected, and to guarantee that such information will be Accessed and Used only as expressly authorized by VDE Controls. (2) At most VDE nodes, the Protected Processing Environment is a Secure Processing Environment . . . (3) The Tamper Resistant Barrier prevents all unauthorized (intentional or accidental) interference, removal, observation, and use of the information and processes within it,

by all parties (including all users of the device in which the Protected Processing Environment resides), except as expressly authorized by VDE Controls." (See JCCS Exh. A at Row 62).

As InterTrust notes, the Big Book describes two categories of processing environment. One, called a Secure Processing Environment (SPE), is hardware-based, centered on the Secure Processing Unit (SPU) with a hardware tamper resistant barrier. This SPE is said to provide "true" security. Another, called a Host Processing Environment (HPE), lacks an SPU, and if it has any tamper resistant barrier, it is software based. The Big Book says that an HPE provides less protection and may not be "truly secure." The patent uses the term "Protected Processing Environment" to refer to either an SPE, or HPE, except as otherwise indicated. And, it says that an HPE may be "secure" or "non-secure." (Alexander Dec. Exh. D at 16(C), 16(H), 16(I), 18(A)-18(E).)

The same three reasons cited above for "tamper resistant barrier" also demonstrate that these claims' "protected processing environment" must be the hardware-based Secure Processing Environment, not the software-based Host Processing Environment.

**InterTrust's Proposed Construction**: (1): "An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat . . . ." (See JCCS Exh. A at Row 62).

This definition is vague in several respects. For example, what does it mean to "at least in part protect" processing and/or data? What exactly does the "in part" modify? Does protection mean prevention, or is merely allowing detection good enough as InterTrust suggests for "secure"? And, as the level of protection depends on the threat, what precise threat(s) are assumed by this claim term, and what "level of protection" is required by those threats? And, is the "processing and/or data" inside the environment being protected from the outside world, or is the outside world being protected from what's inside the environment? In any event, InterTrust's proposal again fails to honor any of the requirements of the VDE "invention," including its ability to prevent all unauthorized access, use, observation, and interference.

## XIII. CONSTRUCTION OF "COMPONENT ASSEMBLY"

**Central Dispute**: Whether a "component assembly" is executable.

In the disclosed "invention," "component assemblies" are dynamically created executable components (called VDE's "basic functional unit") which help give VDE its touted flexibility and user-configurability.

**Ordinary Meaning**: The parties agree that the term "component assembly" has no ordinary meaning in this art.

**Microsoft's Construction**: "(1) A cohesive Executable component created by a channel which binds or links together two or more independently deliverable Load Modules ..., and associated data; ...." (See JCCS Exh. A at Row 99).

In the Big Book, the term "component assembly" (also called "component") uniformly is used to refer to executable components, which are an assembly of independent, executable load modules and data. These VDE component assemblies may be transferred between VDE nodes to perform various tasks, and each is "executable." (See Alexander Dec. Exh. D at 24-4(CC), 6(B, C).) The **only** kind of "component assembly" mentioned in these patents is this VDE component assembly.

**InterTrust's Proposed Construction**: "Components are code and/or data elements that are independently deliverable...." There is no support for this notion that a component assembly may be mere non-executable data. None of the above-quotes (e.g., "component assemblies 690 are the basic functional unit") would make any sense if the component assembly were not executable. Indeed, as noted below, the most important executable component in VDE—the VDE control—is a component assembly.

## XIV. CONSTRUCTION OF "CONTROL" (NOUN)

**Central Dispute**: Whether a "control" is an executable component.

Satisfactory execution of "VDE controls" give authorized users access to content protected by VDE secure containers and VDE protected processing environments.

**Ordinary Meaning**: While the term "control" is used frequently in computer science, it does not have any precise ordinary meaning, but rather means different things in different contexts.

**Microsoft's Construction**: "(1) Independent, special-purpose, Executable, which can execute only within a Secure Processing Environment. (2) Each VDE Control is a Component Assembly dedicated to a particular activity (e.g., editing, modifying another Control, a user-defined action, etc.), particular user(s), and particular protected information, and whose satisfactory execution is necessary to Allowing ... that activity...." (See JCCS Exh. A at Row 4).

VDE "controls" can be explained, partially, with an analogy to a rare books library holding valuable texts. Each different type of access and use of these texts is controlled by a different set of rules, and possibly a different guard or librarian. One guard checks one list of permitted visitors to enter the library; another may check a shorter list for entry to a particular room with particularly valuable texts; another librarian will follow other rules to collect certain texts and supervise their viewing; another may follow other rules to determine whether the visitor may copy any portion of the text; and another may need to authorize or stay after hours to translate (decrypt) the text, or perhaps only particular pages thereof. In VDE, these separate guards and librarians are independent, executable VDE controls which, based on applicable rules, allow a particular type of access or use, and then monitor that access or use. Prof. Maier's explanation of VDE explains an example of these independent VDE controls in operation.

The Big Book states that an important feature of VDE is that each VDE control specializes in allowing and supervising only one type of access or use. VDE controls independently govern separate activities (e.g., access or copy or read); independently govern arbitrarily small portions of data; and are configurable by all participants (subject only to other participants' controls).

> "**Secure electronic controls** can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners, can only be viewed and will be 'destroyed' after a certain elapse of time or real time or after a certain number of

handlings, etc.) **Persistent secure electronic controls** can continue to supervise item workflow even after it has been received and 'read.'" ('683 6:18 - 9:4)

**InterTrust's Proposed Construction**: InterTrust's proposed construction of "Control" again ignores the Big Book in favor of a vague, non-VDE construction: "Information and/or programming Governing operations on or use of Resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations." (See JCCS Exh. A at Row 4). With its "information and/or programming" language, InterTrust suggests that a "control" may be mere non-executable information. More specifically, InterTrust has equated non-executable "rules" and executable "controls." This confuses the guard (control) with the rules he or she follows in allowing and monitoring certain accesses or uses. In the Big Book's usage, a "rule" need not be executable, but a "control" must be.

InterTrust argues that "rules and controls" are equated with "control information," and control information may be mere data, and therefore a control may be mere data. But, under that "logic," apples may be oranges because a sentence in a text reads "apples and oranges (fruit)." The patents do not equate rules and controls, but rather distinguish them by, e.g., often referring to "rule **and/or** control":

> "...at least one **rule and/or control** associated with the software agent that governs the agent's operation." ('193 241:2-3)
>
> "If necessary, trusted go-between 4700 may obtain and register any methods, **rules and/or controls** it needs to use or manipulate the object 300 and/or its contents (FIG. 122 block 4778)." ('683 47:42-45)

Just as it makes no sense to refer to "apple and/or apple," it would make no sense to refer to "rule and/or control" if they were the same.

## XV. CONSTRUCTION OF SOME OTHER TERMS AND PHRASES

"A budget specifying the number of copies which can be made of said digital file" (JCCS Exh. A at Row 6): InterTrust's proposed construction refers to a budget "stating the number of copies that can be made of the digital file," without specifying "can be made since when?" or "by

whom?" or "by what?" Microsoft's construction answers these open questions. (See also Reiter Depo. at 267:18-268:15.)

"Container" (JCCS Exh. A at Row 57): InterTrust proposes that a "container" "means a digital file containing linked and/or embedded items." Prof. Reiter, however, could think of no non-empty digital file which did not "contain linked and/or embedded items," and thus all digital files would qualify as "containers." That is not how this term is used in InterTrust's patents. (See Alexander Decl. Exh. D at 20(A-D).)

"Containing" (JCCS Exh. A at Row 58): The parties disagree on whether storing an indication of where an element may be found, constitutes "containing" that element. The patents are internally inconsistent on this; sometimes saying that "referencing" something is "containing" it; and other times indicating that "referencing" something is an alternative to "containing" it. (See, e.g., Alexander Decl. Exh. D at 24-8(I) ("containing or referencing").) As the normal, ordinary meaning of "contain" is to include within, not reference, the Court should adopt that meaning.

"Controlling" (JCCS Exh. A at Row 7): InterTrust's proposed construction of "control" as a verb is typically vague: "to exercise authoritative or dominating influence over; direct." This loose "influence" of the sort pertinent to persons, not computers, is not what the Big Book promises the owners of content entrusted to VDE. They were promised strict control (including monitoring) over all access and uses, including the ability to prevent (not merely detect) unauthorized access and use. (See Reiter Depo. at 165:3-9.)

Moreover, "controlling" in this "invention" is done at an arbitrary granularity, which is an important feature that the Big Book relied upon to distinguish prior art:

> **"VDE also** extends usage control information to an arbitrary granular level **(as opposed to a file based level provided by traditional operating systems)"**

(See Alexander Decl. Exh. D at 24-4(X) ('193 275:8-11)).

"Controlling the copies made of said digital file" (JCCS Exh. A at Row 7): Whereas the claim refers to "controlling the copies," InterTrust reads the claim more as "controlling the

copying." Also, InterTrust's proposal suggests that the copies are transferred to the second device, but the claims recite that the file (as opposed to any copy) is transferred.

"Derives information from one or more aspects of said host processing environment" (JCCS Exh. A at Row 92): Prof. Reiter links this claim language to the "machine signature" technique described in the '900 Patent. That technique derives a "unique" signature of an appliance so that the HPE-forming software will not run on any other appliance. InterTrust's proposed construction lacks this "unique machine signature" technique. Under InterTrust's proposed construction, the derived information may serve no security purpose at all, which again is contrary to the patent.

"Host Processing Environment" (JCCS Exh. A at Row 87): The Big Book states that a "Host Processing Environment" may be secure or not secure. InterTrust's proposed construction requires security, and thus is contrary to the Big Book. Microsoft's construction explains what it means in the Big Book for a "host processing environment" to be non-secure.

"Identifying (Identify)" (JCCS Exh. A at Row 28): In common usage and these patents, to identify someone or something is to establish the person or thing as a particular individual or thing. InterTrust tries to expand this common understanding with its proposal: "establishing the identity of or to ascertain the origin, nature, or definitive characteristics of; ...." This is contrary to the ordinary meaning, and, again, too vague. Is gray hair a "definitive characteristic" of a person? Is a particular manufacturer of a device sufficient to establish its "nature?" The jury and public would have to guess.

"Tamper Resistance" (JCCS Exh. A at Row 67): InterTrust's proposed construction, "Making tampering more difficult and/or allowing detection of tampering," suffers from the same type of defects as InterTrust's other proposals. For example, "more than difficult than what?" Also, merely detecting tampering but not stopping it, plainly is not what VDE means by "tamper resistance."

For the foregoing reasons, Microsoft's proposed constructions should be adopted.

Dated: April 7, 2003

By: _____
ERIC L. WESENBERG